修 士 論 文 の 和 文 要 旨

大学院　情報システム学研究科　　博士前期課程　情報システム運用学専攻		
氏　　名	浅沼　格	学籍番号 0452001
論　文　題　目	ローカルエリアネットワーク監視のための視覚化システム	

要　　旨

近年の不正アクセスやワームなどのサイバー攻撃の増加に伴い，ネットワーク型不正侵入検知システム(NIDS)によるネットワーク監視が重要視されている．NIDSの利用はセキュリティレベルを向上させるだけでなく，監視により得られたログデータを分析することにより，ワームやウイルスの流行や特性を発見する材料となる．これらのログデータは非常に膨大であり，目視での解析はネットワーク管理者の負担が大きいため，監視結果を地図や表で表すシステムや，ログデータを計算機画面に視覚化する手法が数多く提案されてきた．それらは主に攻撃の時間推移や統計量，攻撃と地理的情報の関係などを表現しているものがほとんどであり，多くは外部ネットワーク監視のためものであった．

一方，組織内のネットワークでのポリシー違反や不正な行為を監視する重要性が高まってきている．そこで本研究では実際にネットワーク調査を行いLANに存在する脆弱性について検証を行い，その結果を利用してLAN監視のための視覚化システムの開発を行った．

本視覚化システムはポートスキャンツールにより得られるOSやサービスの状況などのLANの脆弱性を含むデータと，NIDSにより検知された攻撃情報をリアルタイムで統合し視覚化するシステムである．まずネットワーク調査により得られたデータをLAN内部に存在するホストのポートの状況やOSの種類などにより分類し，それぞれを広域監視システムであるIP Matrixの視覚化手法で表示をする．そしてネットワークの入り口に設置したNIDSのログデータをリアルタイムで同様にマトリクス表示し，それら複数の図を同時に比較することにより，受けた攻撃が本当に脅威であるのかどうかをある程度判断することが出来る．また，攻撃をOS情報やポート番号でフィルタリングすることにより無効な攻撃の表示を省き，目的とする情報のみをネットワーク全体の状況と共に表示できるようにした．これらの機能により，LAN内でBOTに感染したホストを発見することができた．